Gerhard Eschelbeck
CTO and VP Engineering
Qualys

BlackHat Conference Japan
October 2004
Agenda

- Evolution of Threats
- Research Methodology
- One Year After: Update on the External Data
- The Internal Data
- The Laws of Vulnerabilities
- Summary and Action
The worm.sdsc.edu Project

- Experiment: Attaching and monitoring a “default installed” system on the Internet
- Within 8 hours first probe for rpc vulnerabilities was detected
- Within a few days over 20 exploit attempts
- Within a few weeks the system was completely compromised and a network sniffer was installed by an attacker
Exploiting Systems is Getting Easier

- **Weakening Perimeters**
  - Multiple entry points
  - Wireless and VPN connectivity points

- **Increasing complexity of networks and applications**
  - Thousands of exploitable vulnerabilities
  - Shortage of qualified security staff

- **Increasing sophistication of attacks**
  - Simple and automated attack tools
  - Designed for large scale attacks
  - Attack sources hard to trace
Where are the issues?

- A Multitude of insecure Protocols and Services
  - telnet, ftp, snmp

- Known default settings
  - Passwords, SNMP community strings

- System Design Errors
  - Setup and Access control errors

- Software Implementation Flaws
  - Input validation, lack of sanity checks

- User Triggered Issues
  - Email and Browser related
First Generation Threats

- Spreading mostly via email, file-sharing
- Human Action Required
- Virus-type spreading / No vulnerabilities
- Examples: Melissa Macro Virus, LoveLetter VBScript Worm
- Replicates to other recipients
- Discovery/Removal: Antivirus
What happened since then?

- Security flaws in all relevant software packages
- 40 new vulnerabilities per week
- Internet Explorer: 100+ vulnerabilities
- 802.11 wireless security broken
- Successful attacks against the Internet root DNS servers
- Popularity of the “Port 80 Loophole”
- Major worm outbreaks
Second Generation Threats

- Active worms
- Leveraging known vulnerabilities
- Low level of sophistication in spreading strategy (i.e. randomly)
- Non Destructive Payloads
- Blended threats (consists of virus, trojan, exploits vulnerabilities, automation)
- System and Application level attacks
- Remedy: Identify and Fix Vulnerabilities
Windows Vulnerabilities in Action: The Outbreak of the SQL Slammer Worm

Packet Loss %

- Global Paths (1389)
- Global ISP1000 (693)
- DNS servers (302)
- Global Web (731)
- Global Internet (2464)

Timezone (GMT/EST): Jan 24 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00

Jan 24 7 PM 9 PM 11 PM Jan 25 3 AM 5 AM 7 AM 9 AM 11 AM 1 PM 3 PM

(c) Copyright 2003 Matrix NetSystems, Inc. www.matrixnetsystems.com

The Laws of Vulnerabilities

9
What’s Next?

- Improved speed and strategy to identify new vulnerable targets
- Popularity of the exploited system/application/platform
- Affecting New Technologies/Applications
- Shortening Vulnerability/Exploit Life-Cycle
Vulnerability and Exploit Lifecycle

Everyone A Target At This Stage…
Third Generation (Future) Threats

- Leveraging known and unknown vulnerabilities
- Precompiled list of initial victims to provide aggressive growth
- Active Payloads
- Leveraging polymorphic techniques and encryption to prevent discovery
- Multiple attack vectors
- Impact on new Technologies (Instant Messaging, Wireless Networks, Voice over IP,...)
Firewalls and IDS are not protecting

- **Enforcement (Firewalls)**
  - Structuring at the network level – building security zones
  - Limited visibility at application level
  - Mostly static in decision making

- **Secure Transport (VPN)**
  - Expanding corporate networks into the Internet

- **Monitoring (IDS)**
  - Limited scope of data for decision making
  - Massive amounts of log/report information
  - Mostly reactive
Research

- Objective: Understanding prevalence of critical vulnerabilities over time in real world
- Timeframe: January 2002 - Ongoing
- Data Source:
  - 70% Global Enterprise networks
  - 30% Random trials
- Methodology: Automatic Data collection with statistical data only – no possible correlation to individual user or systems
External and Internal Data Sources

The graph shows the comparison of internal and external data sources over time. The y-axis represents the number of data points, and the x-axis represents time from January 2002 to May 2004. The graph highlights two significant events:

- **Sasser Worm**: Internal data points show a significant increase in May 2003.
- **Blaster Worm**: Internal data points show a significant increase in April 2004.

The graph indicates a decrease in external data points during these events, as indicated by the blue bars.
Raw Results

- Largest collection of global real-world vulnerability data:
  - 6,627,000 IP-Scans since begin 2002
  - 2,275 out of 3,374 unique vulnerabilities detected in the real world
  - 3,834,000 total critical* vulnerabilities found
  - 1,031 out of 1,504 unique critical vulnerabilities detected in the real world

* Providing an attacker the ability to gain full control of the system, and/or leakage of highly sensitive information. For example, vulnerabilities may enable full read and/or write access to files, remote execution of commands, and the presence of backdoors.
Analysis Performed

- Identifying Window of Exposure
- Lifespan of Critical Vulnerabilities
- Resolution Response
- Trend over Time
- Vulnerability Prevalence
Microsoft WebDAV Vulnerability

Microsoft Windows 2000
IIS WebDAV Buffer Overflow Vulnerability

CAN-2003-0109
Qualys ID 86479

Released: March 2003
Vulnerability Half-Life

2003: For a critical vulnerability every 30 days the number of vulnerable systems is reduced by 50%
Microsoft WebDAV Vulnerability

Microsoft Windows 2000
IIS WebDAV Buffer Overflow Vulnerability
CAN-2003-0109
Qualys ID 86479
Released: March 2003
WU-FTPd File Globbing Heap Corruption Vulnerability

CVE-2001-0550
Qualys ID 27126
Released: November 2001
Microsoft Windows ASN.1 Library Integer Handling Vulnerability

Microsoft Windows ASN.1 Library Integer Handling Vulnerability
CAN-2003-0818
Qualys ID 90103
Released: February 2004
Buffer overflow in Microsoft Local Security Authority Subsystem Service (LSASS)

Buffer overflow in Microsoft Local Security Authority Subsystem Service (LSASS)

CAN-2003-0533
Qualys ID 90108
Released: April 2004
2004: For a critical vulnerability every 21 days the number of vulnerable systems is reduced by 50%
Microsoft Exchange Server Buffer Overflow Vulnerability

Microsoft Exchange Server Buffer Overflow Vulnerability
CAN-2003-0714
Qualys ID 74143
Released: October 2003
Microsoft Messenger Service Buffer Overflow Vulnerability

Microsoft Messenger Service Buffer Overflow CAN-2003-0717
Qualys ID 70032
Released: October 2003
For a critical vulnerability every 21 days (62 days on internal networks) 50% of vulnerable systems are being fixed.
SSL Server Allows Cleartext Communication

SSL Server Allows Cleartext Communication
Qualys ID 38143
SQL Slammer Vulnerability

MS-SQL 8.0 UDP
Slammer Worm Buffer Overflow Vulnerability

CAN-2002-0649
Qualys ID 19070
Released: July 2002
A Continuous Cycle of Infection
Vulnerability Lifespan

The lifespan of some vulnerabilities and worms is unlimited.
The Sasser Worm and its Victims

Buffer overflow in Microsoft Local Security Authority Subsystem Service (LSASS)

CAN-2003-0533
Qualys ID 90108
Released: April 2004
The Impact of an Exploit

80% of worms and automated exploits are targeting the first two half-life periods of critical vulnerabilities.
Mapping Vulnerability Prevalence

Vulnerability Prevalence

Individual Vulnerabilities
The Changing Top of the Most Prevalent

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>CVE</th>
<th>Jul-02</th>
<th>Jan-03</th>
<th>Jul-03</th>
<th>Jan-04</th>
<th>Jul-04</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache Mod_SSL Buffer Overflow Vulnerability</td>
<td>CVE-2002-0082</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Exchange 2000 Malformed Mail Attribute DoS Vulnerability</td>
<td>CVE-2002-0368</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Index Server and Indexing Service ISAPI Extension Buffer Overflow Vulnerability</td>
<td>CVE-2001-0500</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft IIS FTP Connection Status Request Denial of Service Vulnerability</td>
<td>CVE-2002-0073</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft IIS Chunked Encoding Transfer Heap Overflow Vulnerability</td>
<td>CVE-2002-0079</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft IIS HTR ISAPI Extension Heap Overflow Vulnerability</td>
<td>CVE-2002-0364</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft IIS 4.0.5.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft IIS CGI File Manager</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft IIS Malformed Mail Attribute DoS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft IIS HTR CGI Server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apache Chunked-Encoded Transfer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OpenSSH Challenge Authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multiple Vendor SHM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISC BIND SIG Cache</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows 2000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sendmail Address Previous Possible Memory Corruption Vulneribility</td>
<td>CAN-2003-0151</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft SMB Request Handler Buffer Overflow Vulnerability</td>
<td>CAN-2003-0345</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability</td>
<td>CAN-2003-0352</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft DCOM RPCSS Service Vulnerability</td>
<td>CAN-2003-0528</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Messenger Service Buffer Overrun Vulnerability</td>
<td>CAN-2003-0717</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Buffer Overflow In Microsoft Local Security Authority Subsystem Service (LSASS)</td>
<td>CAN-2003-0533</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft RPCSS Code Execution Variant</td>
<td>CAN-2003-0813</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows ASN.1 Library Integer Handling Vulnerability</td>
<td>CAN-2003-0818</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

50% of the most prevalent and critical vulnerabilities are being replaced by new vulnerabilities on an annual basis.
# Top 10 External (Most Prevalent and Critical Vulnerabilities) as of October 14, 2004

<table>
<thead>
<tr>
<th>Title</th>
<th>Qualys ID</th>
<th>CVE Reference</th>
<th>External Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache Chunked-Encoding Memory Corruption Vulnerability</td>
<td>86352</td>
<td>CVE-2002-0392</td>
<td>CA-2002-17</td>
</tr>
<tr>
<td>Microsoft Windows 2000 IIS WebDAV Buffer Overflow Vulnerability</td>
<td>86479</td>
<td>CAN-2003-0109</td>
<td>MS03-007</td>
</tr>
<tr>
<td>Microsoft Windows DCOM RPCSS Service Vulnerabilities</td>
<td>68522</td>
<td>CAN-2003-0528</td>
<td>MS03-039</td>
</tr>
<tr>
<td>Buffer overflow in Microsoft Local Security Authority Subsystem Service (LSASS)</td>
<td>90108</td>
<td>CAN-2003-0533</td>
<td>MS04-011</td>
</tr>
<tr>
<td>Buffer Management Vulnerability in OpenSSH</td>
<td>38217</td>
<td>CAN-2003-0693</td>
<td>CA-2003-24</td>
</tr>
<tr>
<td>Microsoft Windows RPCSS Code Execution Variant</td>
<td>68528</td>
<td>CAN-2003-0813</td>
<td>MS04-012</td>
</tr>
<tr>
<td>Microsoft Windows ASN.1 Library Integer Handling Vulnerability</td>
<td>90103</td>
<td>CAN-2003-0818</td>
<td>MS04-007</td>
</tr>
<tr>
<td>SSL Server Allows Cleartext Communication Vulnerability</td>
<td>38143</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Writeable SNMP Information</td>
<td>78031</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
## Top 10 Internal (Most Prevalent and Critical Vulnerabilities) as of October 14, 2004

<table>
<thead>
<tr>
<th>Title</th>
<th>Qualys ID</th>
<th>CVE Reference</th>
<th>External Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft SQL Weak Database Password</td>
<td>19001</td>
<td>CAN-2000-1209</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability</td>
<td>68518</td>
<td>CAN-2003-0352</td>
<td>MS03-026</td>
</tr>
<tr>
<td>Microsoft Windows DCOM RPCSS Service Vulnerabilities</td>
<td>68522</td>
<td>CAN-2003-0528</td>
<td>MS03-039</td>
</tr>
<tr>
<td>Buffer overflow in Microsoft Local Security Authority Subsystem Service (LSASS)</td>
<td>90108</td>
<td>CAN-2003-0533</td>
<td>MS04-011</td>
</tr>
<tr>
<td>Microsoft Messenger Service Buffer Overrun Vulnerability</td>
<td>70032</td>
<td>CAN-2003-0717</td>
<td>MS03-043</td>
</tr>
<tr>
<td>Microsoft Windows Workstation Service Remote Buffer Overflow Vulnerability</td>
<td>90078</td>
<td>CAN-2003-0812</td>
<td>MS03-049</td>
</tr>
<tr>
<td>Microsoft Windows RPCSS Code Execution Variant</td>
<td>68528</td>
<td>CAN-2003-0813</td>
<td>MS04-012</td>
</tr>
<tr>
<td>Microsoft Windows ASN.1 Library Integer Handling Vulnerability</td>
<td>90103</td>
<td>CAN-2003-0818</td>
<td>MS04-007</td>
</tr>
<tr>
<td>Microsoft Outlook Express Cumulative Security Update not installed</td>
<td>90110</td>
<td>CAN-2004-0380</td>
<td>MS04-013</td>
</tr>
<tr>
<td>Microsoft Internet Explorer Cumulative Security Update not installed</td>
<td>100008</td>
<td>CAN-2004-0549</td>
<td>MS04-025</td>
</tr>
</tbody>
</table>
The Laws of Vulnerabilities

1. Half-Life
   The half-life of critical vulnerabilities is 21 days on external systems and 62 days on internal systems, and doubles with lowering degrees of severity

2. Prevalence
   50% of the most prevalent and critical vulnerabilities are replaced by new vulnerabilities on an annual basis

3. Persistence
   The lifespan of some vulnerabilities and worms is unlimited

4. Exploitation
   The vulnerability-to-exploit cycle is shrinking faster than the remediation cycle. 80% of worms and automated exploits are targeting the first two half-life periods of critical vulnerabilities
Goal: Shortening the Half-Life of Critical Vulnerabilities for Internal systems to 40 days
Summary and Actions we can take:

- Significant progress on the Remediation Cycle (30 to 21 days) for external Vulnerabilities

- Goal: Shortening the Half-Life of internal vulnerabilities from 62 days to 40 days within one year

- Required: Your support to reach this goal

- References:
  - [http://www.qualys.com/laws](http://www.qualys.com/laws) This presentation and any future updates
  - [http://www.qualys.com/top10](http://www.qualys.com/top10) Continuously updated Top Ten Index of most prevalent and critical external and internal vulnerabilities
  - [http://www.qualys.com/top10scan](http://www.qualys.com/top10scan) Free Top Ten Assessment Tool

- Comments and Suggestions: geschelbeck@qualys.com